Cyber Intelligence: Challenges and Best Practices

Emerging Technology Center

Samantha L. Allen

January 2015

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
15 JAN 2015	**N/A**	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cyber Intelligence Challenges and Best Practices	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Allen /Jay McAllister Samantha	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**26**	

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0002107

Agenda

Cyber Intelligence Tradecraft Project

Challenges and Best Practices

Cyber Intelligence Research Consortium

Cyber Intelligence Tradecraft Project

Sponsor

- National Intelligence Manager for Cyber, Office of the Director of National Intelligence (ODNI)

Purpose

- Study how organizations from industry, government, and academia perform cyber intelligence (methodologies, processes, tools, and training)

Definition of cyber intelligence

- The acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions, and activities to offer courses of action that enhance decision making

Overall finding

- The most effective organizations balanced the need to protect their network perimeters with the need to look beyond them for strategic insights

Challenges

&

Best Practices

Q: How do you do cyber intelligence?

"We try to mirror the traditional intelligence cycle."

- US government participant

Stale processes

Traditional Intelligence Cycle

Image source: ODNI - http://www.dni.gov/index.php/newsroom/reports-and-publications/193-reports-publications-2013/835-u-s-national-intelligence-an-overview-2013-sponsored-by-the-intelligence-community-information-sharing-executive

Reporting timelines

	Urgent	Normal	Strategic
Gov't Agency 1	2-4 Hours	1 Day	1 Month
Gov't Agency 2	1 Day	2 Weeks	3 Months
Gov't Agency 3	1 Day	3 Months	***6 – 18 Months***
Gov't Agency 4	2 Hours	8 Hours	5 Days

Success using nonlinear, interactive conceptual frameworks

Analytical Acumen

- Facilitates timely/actionable/accurate intelligence

Environmental Context

- Provides scope for the analytical effort

Data Gathering

- Acquires and aligns data for analysis

Microanalysis

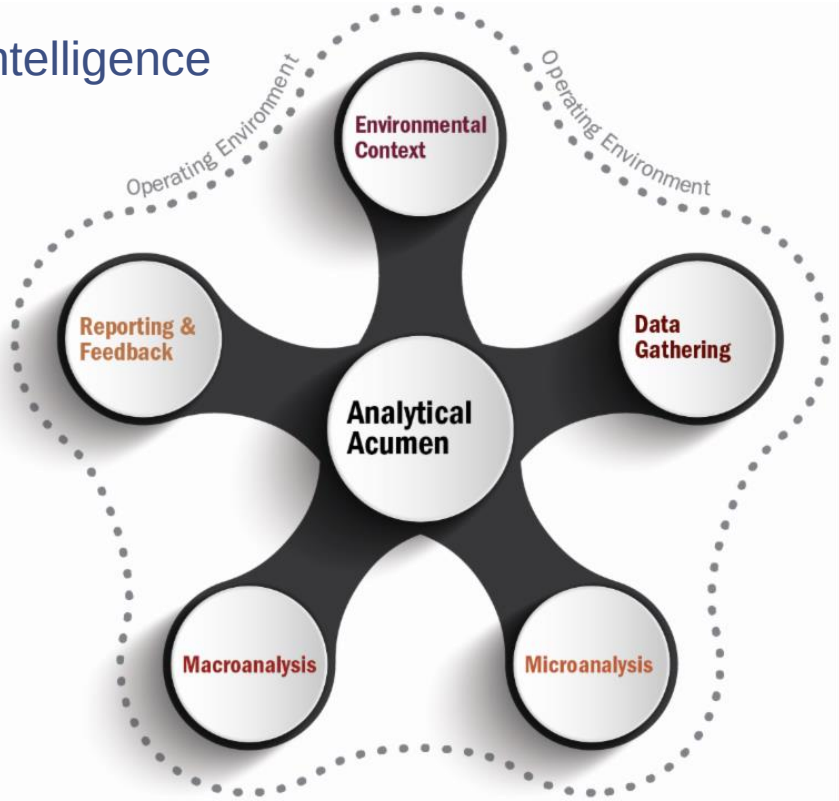
- Assesses functional implications

Macroanalysis

- Assesses strategic implications

Reporting and Feedback

- Offers courses of action to enhance decision making



Q: How do you rank threats, from high to low?

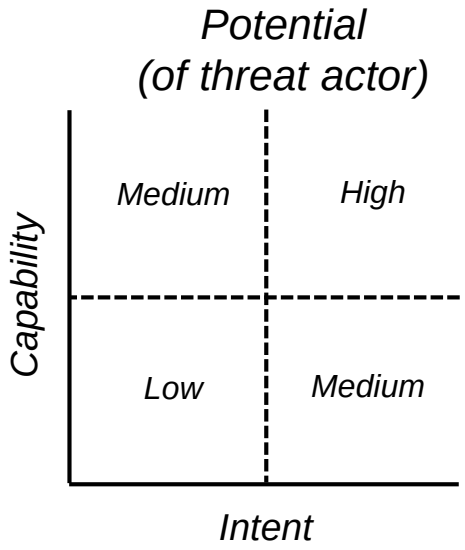
"We consider everything a high priority threat."

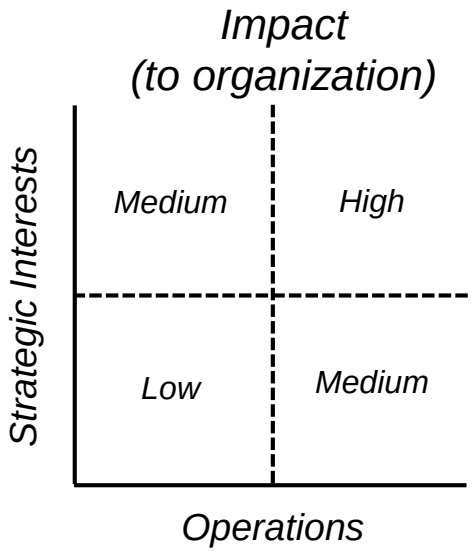
- US government participant

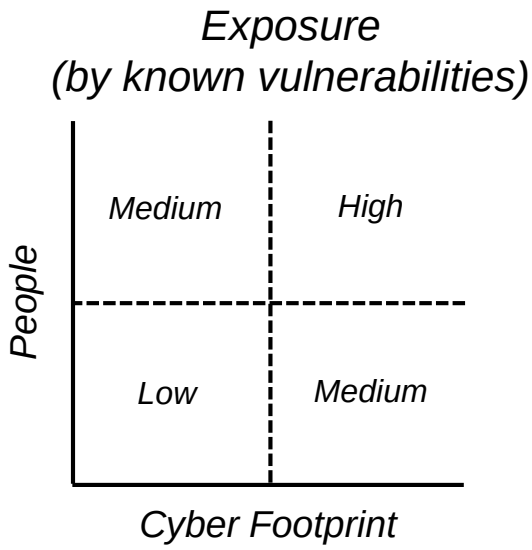
Stale processes

Threat prioritization

Implementing…
Threat = Potential + Impact + Exposure







Threat Actor Potential
(to execute the cyber threat)

Capability

Attack Methods

- **Infrastructure**
  Operational structures needed for success—hardware, software, or command and control
- **Technology**
  Whether used or manipulated
- **Coding**
  Nuances and personal preferences
- **Maturity**
  According to the planning process and pre/post-threat activities
- **Targets**
  General or specific—mass phishing data or exploiting a specific vulnerability
- **Timing**
  Minutes, days, or years to act on the cyber threat

Resources

- **Money**
  For personnel, tools, training, or access
- **People**
  Number and type of people involved—collaborators, teachers, mentors, or sponsors
- **Tools**
  Open source and/or custom, and why
- **Training**
  Type and quality

Intent

Motive

- **Intrinsic**
  Personal rewards to act on the threat—bragging rights, knowledge, justify skills, satisfy boredom, patriotism, or hacktivist allegiance
- **Extrinsic**
  External rewards to act on the threat—fame, money—or to avoid punishment

Targeted Data

- **Personally Identifiable Information (PII)**
  Payment card data, social security numbers, or biometrics
- **Organizational Data**
  Research and development information, business processes, or industrial control systems

Organizational Impact
(of the cyber threat on the target)

Operations

Direct Costs

Incident Response
Costs to perform an investigation, remediation, and forensics

Downtime
Business costs of a network-reliant service being unavailable—missed financial transactions or loss of potential product/services revenue

Mitigation and/or Prevention
Costs of additional hardware/software to stop current and future threats

Business Operations

Supply Chain
Costs associated with the inability to meet demand, delay to operations, and supplementing or replacing suppliers

Logistics
Cost of continuing business operations during and after an attack—rerouting communications, securing intellectual property, or upgrading processes

Future Earnings
How the threat affects R&D, product releases, acquisitions, or competitive advantage

Strategic Interests

Organizational Interests

Strategic Planning
How the threat affects the strategic vision—annual reports, operational policies, or mergers

Stakeholders
Threat impact on shareholders, board of directors, or employees

Culture
How the threat affects legal/regulatory requirements, network access, or work-from-home policies

External Interests

Market/Industry
Threat impact on target's competitors and industry, both domestic and foreign

Geopolitical
How the threat affects political relationships and local/national/global economies

Partnerships
Threat impact on target's third party providers, information sharing agreements, or other business relationships

Brand Reputation
How the threat affects the target's brand and its implications on public opinion

Target Exposure
(to the cyber threat because of potential vulnerabilities)

People

Relevance

Internet Presence
Susceptible witting and unwitting information target-related individuals put online and their popularity on blogs/social media

Extracurricular Activities
Vulnerabilities from these individuals roles with non-target entities—non-profits, activist groups, or local/national politics

Motive
The reasons for why such individuals are susceptible to the cyber threat—ignorance, financial trouble, disgruntlement, or boredom

Access

Physical
Vulnerabilities from target-related individuals ability to access the target's tangible aspects—office space, transportation, or equipment

Network
Susceptible administrative privileges or sensitive data access provided to such individuals

Position
How threat actors exploit the different roles these individuals play for the target—network administrator, senior leader, or rank-and-file employee

Abnormal Activities
Deviations from normal physical, network, or position-based activities of key target-related individuals can signify potential vulnerabilities

Cyber Footprint

Infrastructure

Hardware
Risks emanating from where network appliances, workstations, and third party equipment connect to the target's network

Software
Risks associated with the target relying on particular software for day-to-day operations, providing access to high-risk software, and detecting software vulnerability exploitation

Supply Chain
How the cyber threat affects the target's acquisition, implementation, maintenance, and discontinuation of hardware and software

Internet Presence

Website
How the threat actor can leverage the target's website—compromise content, collect data, or deny access

Social Media
Risks associated with the target's use of it for organizational activities—marketing, customer service, or product placement

Additional Services
Risks emanating from the target's use of FTP, Telnet, VPN, webmail, remote desktop, and other web-based services

Q: Where do your decision makers generally get their cyber intelligence?

"CNN."

- Financial sector participant

Stale processes | Threat prioritization | **Communicating to decision makers**

Validity of cyber intelligence partnerships

Cyber Intelligence Partnership

Business Intelligence
and
Cyber Intelligence Program

Q: How do you demonstrate return on investment?

"We don't."

- Energy sector participant

Stale processes | Threat prioritization | Communicating to decision makers | **Return on Investment**

Compare and contrast for ROI

Image source: https://www.youtube.com/watch?v=X1Tqbd1mi_U

Q: Can you describe your data collection process?

"It's an absolute mess…"

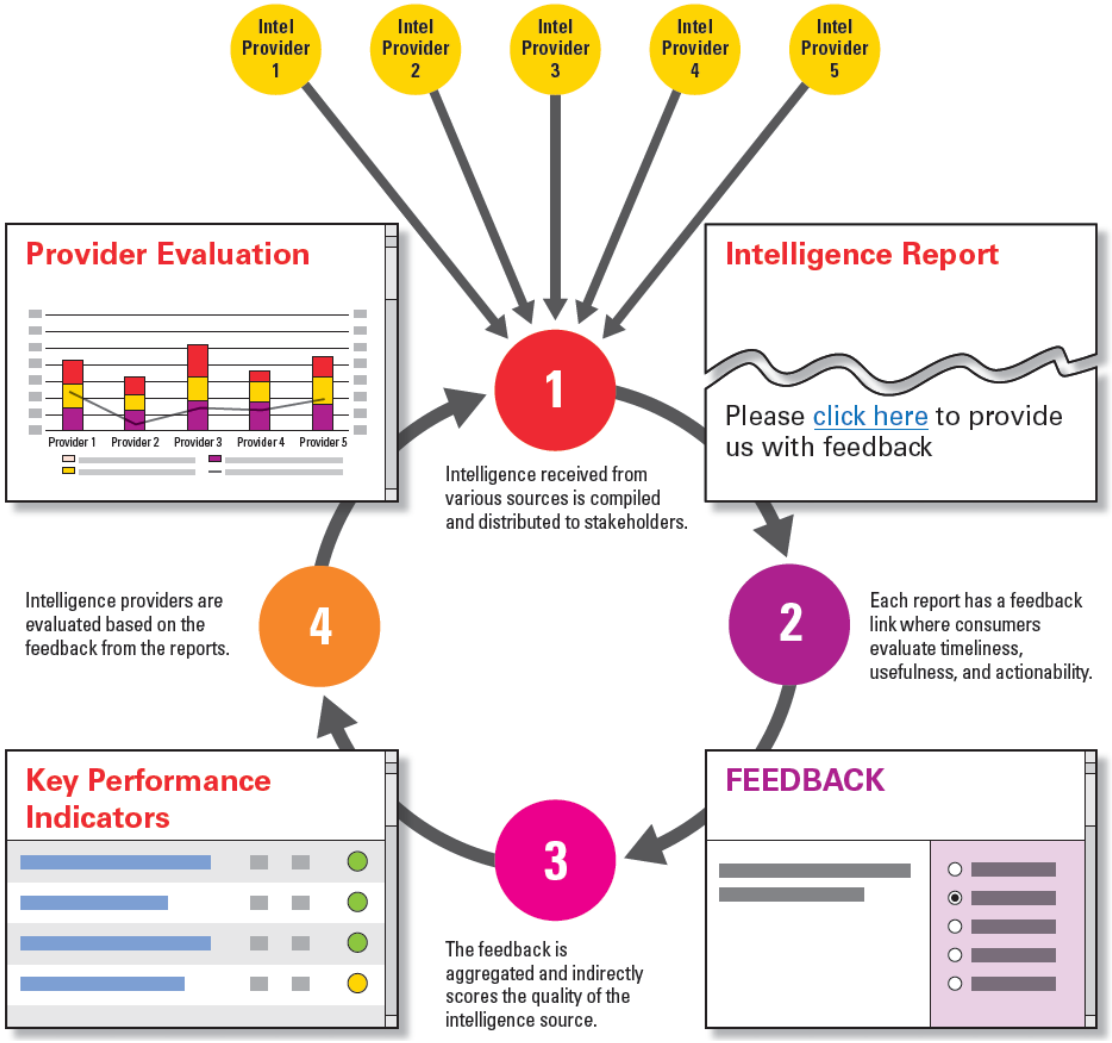
- Energy Sector Participant

Stale processes | Threat prioritization | Communicating to decision makers | Return on Investment | **Collection management**

Levels of collection management

	Basic	Established	Advanced
Requirements	• Establish collection mechanisms • Identify stakeholders	• Add rigor: Not all requests are created equal • Classify requirements • Track requirements	• Incorporate needs of all stakeholders • Continually validate requirements
Operations	• Know your data sources • Know your information gaps • Align data with requirements	• Assess and manage sources • Validate data quality and reliability • Ensure redundancies exist for data coverage	• Validate and evaluate third party information • Look beyond network data • Let intelligence drive data collection • Leverage tipping/queuing
Analysis & Reporting	• Collect data, fuse sources • Add context and calculated judgments/predictions	• Corroborate information with multiple sources • Ensure priority requirements are being met with the available data sources	• Anticipate requirements • Automate analysis of known threats

Establishing an evaluation cycle



Is that it?

Evaluating Intelligence

Challenge

- Cyber intelligence is a phrase often used, but interpreted in many different ways, leading to a diverse output of threat analysis categorized as cyber intelligence
- Such output is difficult to evaluate and compare, stifling an organization's ability to establish guidelines and goals

Solution

- An evaluation template based on standards observed during our research and set forth in U.S. Intelligence Community Directive Number 203
  - http://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards%20pdf-unclassified.pdf

Template – Evaluating Intelligence

Assess the quality and thoroughness of an intelligence analyst's work using a grading system based on points accumulated for criteria the analyst satisfies in an intelligence product

Grading system

A: 17-16, **B:** 15-14, **C:** 13-12, **D:** 11-10, **F:** 9 and below

Criteria

- Objective
- Independent of political considerations
- Timely
- Based on all available sources
- Exhibiting proper standards of analytic tradecraft

Cyber Intelligence Research Consortium

Purpose

- Research and develop technical solutions and analytical practices to help people make better judgments and quicker decisions with cyber intelligence

Membership

- Decision makers and practitioners from academia, Department of Defense, defense contracting, energy, financial services, and the U.S. Intelligence Community

Offerings

- Cyber threat baseline: Threat environment research to identify best practices
- Tradecraft labs: Workshops to advance analytical & technological capabilities
- Implementation frameworks: How-to guides for key intelligence practices
- Crisis simulation: Capture-the-flag exercise to apply techniques & technologies
- Intelligence insights: Continuous communication on relevant topics

Questions?

Jay McAllister
412.268.9193
jjmcallister@sei.cmu.edu
@sei_etc

Output from Cyber Intelligence Tradecraft Project

- http://www.sei.cmu.edu/about/organization/etc/citp.cfm

Information on the Cyber Intelligence Research Consortium

- http://www.sei.cmu.edu/about/organization/etc/overview.cfm